IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN RE GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION	C.A. 12-MD-2358 (SLR)
This Document Relates to: All Actions	

OPENING BRIEF IN SUPPORT OF MOTION TO DISMISS OF DEFENDANTS MEDIA INNOVATION GROUP, LLC AND WPP PLC FOR FAILURE TO STATE A CLAIM

MORRIS, NICHOLS, ARSHT & TUNNELL LLP
Rodger D. Smith II (#3778)
Regina S.E. Murphy (#5648)
1201 North Market Street, 18th Floor
P.O. Box 1347
Wilmington, Delaware 19899-1347
(302) 658-9200
rsmith@mnat.com
rmurphy@mnat.com

Attorneys for Defendants Media Innovation Group, LLC and WPP plc

OF COUNSEL:

Douglas H. Meal
Lisa M. Coyle
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
(617) 951-7000

May 1, 2013

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

INTRODUCTION

Defendants Media Innovation Group, LLC ("MIG") and WPP plc ("WPP" and, together, the "Moving Defendants") respectfully move pursuant to Federal Rule of Civil Procedure 12(b)(6) to dismiss for failure to state a claim the claims asserted against them in the Consolidated Class Action Complaint ("the CAC") by named plaintiffs William Gourley, Todd Heinrich and Lynne Krause (together, "Plaintiffs").[1] This is Moving Defendants' Opening Brief in support of that motion.

This multidistrict litigation is the latest in what is now a long line of lawsuits where the plaintiffs seek to make a federal case out of harmless cookies having been set on their computers. Other federal courts confronted with such cookie-related claims have repeatedly dismissed them at the outset of the case. The Plaintiffs in this case, despite their best efforts to paint routine commercial behavior in a nefarious light, allege no facts supporting an inference that their legal rights were violated or that they suffered any economic loss or were otherwise affected *in any way* by the alleged cookie-setting of which they complain, and thus they should fare no better than their unsuccessful predecessors. Indeed, boiled down to its essentials, the CAC's allegations establish nothing more than that the Moving Defendants interacted with Plaintiffs' Safari browsers in precisely the way those browsers were designed to function, and that *Plaintiffs themselves* initiated these harmless interactions. Because the Moving Defendants' unremarkable and innocuous alleged conduct does not satisfy the elements of any of the statutes on which Plaintiffs base their claims, the CAC should be dismissed, with prejudice, pursuant to Fed. R. Civ. P. 12(b)(6) for failure to state a claim upon which relief can be granted.

[1] The fourth plaintiff named in the CAC, Jose M. ("Josh") Bermudez, does not make any allegations in respect of the Moving Defendants. CAC ¶ 11.

STATEMENT OF FACTS

The CAC alleges that the Moving Defendants are companies that serve their clients' online advertisements to commercial websites. CAC ¶¶ 41, 153, 161. According to the CAC, when an internet user wishes to view a website, the user's browser communicates with the website's server and – through what is referred to as a "GET" request – requests that information contained in the webpage be sent to the user's computer. CAC ¶¶ 31, 41. Upon receipt of the user's request, the website server allegedly sends the site's content to the user's computer and instructs the user's browser to send another "GET" request – this time asking a third-party ad-serving company to supply an ad to the website. CAC ¶ 41. Thus, according to Plaintiffs' allegations, internet users see ads based on an intentional interaction between the user's browser (which initiates this interaction) and the third-party ad-serving company. CAC ¶ 41. In connection with this interaction, Plaintiffs claim that certain browser-generated information such as type of browser and operating system, address of first party website, IP address, and screen resolution (the "Browser-Generated Information") is sent by the browser to the website and the ad-serving company so that the webpage and the ads can be properly delivered and displayed on the user's monitor. *See id.* ¶¶ 30-36, 41, 46.

According to the CAC, if the ad-serving company has, prior to this interaction, set a cookie on the browser, then the anonymous alphanumeric value assigned to that cookie (the "Cookie Value") is sent to the ad-serving company along with the Browser-Generated Information when the browser makes the second GET request. *See id.* ¶¶ 45-46.[2] If the ad-serving company has not previously set a cookie on the browser, and if the user's browser is configured to allow a cookie to be set, the ad-serving company may set a cookie on the user's

[2] A "cookie" is essentially a benign piece of data that, upon being sent from an Internet domain to an Internet user's web browser, can be used by the domain to identify the browser.

browser during this interaction. CAC ¶¶ 45, 76. The CAC nowhere alleges that, once set, a cookie *itself* stores or collects information. Rather, even when read in the light most generous to Plaintiffs, the CAC alleges that each time a browser on which a cookie resides visits a website for which the company that set the cookie serves ads, the cookie merely transmits its Cookie Value back to the ad-serving company, and the ad-serving company "associate[s]" the Cookie Value with the Browser-Generated Information it independently received from the browser on that and other occasions. *Id.* ¶¶ 45-46, 205.

Plaintiffs allegedly used the Apple Safari internet browser on their personal computers and mobile electronic devices to visit websites displaying advertisements delivered by the Moving Defendants and, in the course of delivering such advertisements, the Moving Defendants allegedly set cookies on Plaintiffs' browsers. CAC ¶¶ 10, 12-13, 153, 161. Plaintiffs allege that when they visited websites on which the Moving Defendants served ads, the default privacy setting on their Safari browsers was engaged, CAC ¶¶ 10, 12-13, and that such setting (the "Partial-Allowance Setting") purports to block so-called "third-party cookies," *i.e.* cookies from websites other than those directly visited by Plaintiffs. CAC ¶¶ 69-71. The Partial-Allowance Setting, however, does not attempt to block cookies from "third parties" with which the user interacts directly "in some way, including through the submission of a form to the third-party's website server." CAC ¶ 76.

Plaintiffs contend that the cookies the Moving Defendants allegedly set should have been blocked by the Partial-Allowance Setting but were not because the Moving Defendants allegedly employed certain server code described in a February 2012 blog post by a Stanford University researcher (the "Mayer Article"). CAC ¶¶ 74-75, 77, 153-154, 161. As acknowledged in the Mayer Article, however, when an ad delivered to a Safari browser includes an "iframe"

containing an HTML form, and the form is submitted to a domain, the Partial-Allowance Setting *permits the domain to set a cookie on the browser* even though the browser has not visited the domain. Declaration of Lisa M. Coyle, dated May 1, 2013 ("Coyle Decl.") Ex. A at 2-3 (emphasis added); CAC ¶ 76. In other words, according to the Mayer Article – which provides much of the factual basis for Plaintiffs' claims, and is incorporated by reference into the CAC, *id.* ¶ 75 – the Partial-Allowance Setting is actually expressly configured to *allow* cookies to be set in precisely the manner in which the Moving Defendants allegedly set them:

> Apple's cookie blocking policy is less restrictive than many competing browser vendors'. [Among other things], [i]f an HTTP request to a third-party domain is caused by the submission of an HTML form, *Safari allows the response to write cookies*. . . . These *allowances in the Safari cookie blocking policy* enable three potentially undesirable behaviors by advertising networks [one of which is that] *[a] third-party website can use JavaScript to submit a form in an iframe without any user interaction*.

Coyle Decl. Ex. A at 2-3 (emphasis added). *See also* CAC ¶ 75.

Based on these allegations, Plaintiffs claim the Moving Defendants violated the Electronic Communications Privacy Act (the "Wiretap Act"), 18 U.S.C. § 2510 *et seq.*; the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.*; and the Computer Fraud and Abuse Act ("CFAA"). 18 U.S.C. § 1030. Each of these claims should be dismissed for failure to state a claim on which relief may be granted:

- The Wiretap Act claim fails as a matter of law because the Moving Defendants were parties to the alleged communications on which the claim is based and because, in any event, the Moving Defendants did not "intercept" the "contents" of those communications. See *infra* Point I.
- The SCA claim is legally deficient because Plaintiffs have failed to allege any of the following independently necessary elements: (i) "unauthorized access" (ii) to a "facility" through which an "electronic communications service" was provided, (iii) such that the Moving Defendants "thereby" obtained communications not "of or intended for" them (iv) while they were "in electronic storage." *See infra* Point II.
- The CFAA claim fails as a matter of law because Plaintiffs have not alleged that they suffered the statutorily required "loss" as a result of the Moving Defendants' alleged

conduct and because they in any event do not allege that the Moving Defendants acted "without authorization" or "exceed[ed] authorized access," as they must to plead a CFAA claim. *See infra* Point III.

ARGUMENT

I. PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE WIRETAP ACT

The Wiretap Act imposes liability on a person who "intercept[s]" the "contents" of an "electronic communication," 18 U.S.C. § 2511(1)(a)), § 2510(4), but only if that person is not a party to the communication and lacks prior consent from any party to the communication. 18 U.S.C. § 2511(2)(d). Plaintiffs fail to state a claim under this statute because the facts they allege demonstrate that the Moving Defendants were parties to the communications at issue and did not acquire the "contents" of any electronic communication.

A. The Moving Defendants Were Parties To The Alleged Communications

The Wiretap Act is not violated where a communication is acquired by "a party to the communication" or "where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d). *See also In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001) (holding that, where defendant ad-serving company placed a cookie on a browser when the user visited certain websites, the websites were "parties to the communication[s] from plaintiffs and ha[d] given sufficient consent to [the ad-serving company] to intercept them" and defendant was thus not liable under the Wiretap Act).[3] Plaintiffs specifically allege that their browsers communicated *directly* with the Moving Defendants in the

[3] *See also In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 713 (N.D. Cal. 2011) (defendant website cannot be liable under Wiretap Act where plaintiffs' clicks were either a communication to website or to third party ad-serving company requesting that website pass the communication along); *Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (granting motion to dismiss Wiretap Act claim and observing that to hold "that [an online retailer], by receiving an e-mail, intercepted a communication within the meaning of the Wiretap Act would be akin to holding that one who picks up a telephone to receive a call has intercepted a communication . . .").

context of requesting ads: "Upon receiving a 'GET' request from a user seeking to display a particular webpage, the server for that webpage will subsequently respond to the browser, *instructing the browser to send a 'GET' request to the third-party company charged with serving the advertisements for that particular webpage*." CAC ¶ 41 (emphasis added). According to Plaintiffs, the "GET" request that the browser then sends to an ad-serving company includes the Browser-Generated Information, because that information is necessary for the company to display the ad to the browser. *Id.* ¶¶ 30-36, 41, 46.[4]

According to Plaintiffs' own allegations, then, the communications on which their Wiretap Act claim is based – *i.e.*, the Browser-Generated Information – were intentionally directed by Plaintiffs to the Moving Defendants themselves, making it impossible for the Moving Defendants to have violated the Wiretap Act by having received those communications. *See Yunker v. Pandora Media, Inc.*, No. 11-3113, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013) (dismissing Wiretap Act claim where plaintiff sent information directly to defendant, who was thus a party to the communication). Nor would Plaintiffs' Wiretap Act claim fare any better to the extent Plaintiffs might try to predicate it on the communication of the Cookie Values, rather than the communication of the Browser-Generated Information, because the Moving Defendants

[4] Thus, Plaintiffs' conclusory assertion that the Moving Defendants acquired the Browser-Generated Information not directly from Plaintiffs, but rather while it was "in transit from the Class Members' Computing Devices to the web servers of the first party websites the Class Members used their browsers to visit," CAC ¶ 208, is directly contradicted by the detailed factual allegations in the CAC that purport to explain how the alleged interactions between Plaintiffs and the Moving Defendants worked. CAC ¶¶ 27, 41. But even if Plaintiffs had alleged facts showing that the Moving Defendants acquired information while it was being transmitted to first-party websites, which they have not, Plaintiffs' Wiretap Act claim would still fail because it would be "implausible to infer" that websites displaying ads served from the Moving Defendants' domains "have not authorized [the Moving Defendants'] access" because "the very reason clients hire [ad-serving companies]" is to have advertisements delivered to their webpages. *In re Doubleclick*, 154 F. Supp. 2d at 510 (holding statutory exception to the Wiretap Act applied on face of complaint).

by definition were parties to the communication of the Cookie Values. *See, e.g., In re Doubleclick*, 154 F. Supp. 2d at 511-13 (holding that defendant ad-serving company "did not need anyone's authority to access [Cookie Values]" on plaintiffs' browsers because "to the extent cookie identification numbers are electronic communications *at all*," they were the ad-serving company's "internal . . . communications" and thus were both "of" and "intended for" it) (emphasis added).

B. The Moving Defendants Did Not "Intercept" The "Contents" Of Any Communications Under The Wiretap Act

The Wiretap Act defines the term "intercept" to mean the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). "[C]ontents," in turn, is defined as "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). The contents of a communication are limited to "information the user intended to communicate, such as the words spoken in a phone call," and courts have routinely rejected efforts to expand the Wiretap Act to cover mere transactional information about a communication or information about the parties to a communications. *See, e.g., In re iPhone Appl. Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012) (holding that identities of parties to a communication and other call data, including plaintiffs' precise geographic location, are not contents); *United States v. Reed*, 575 F. 3d 900, 916 (9th Cir. 2009) (holding that data about a telephone call, including time of origination, duration, source and destination are not contents).

According to the CAC, the Browser-Generated Information is sent to the Moving Defendants each time a user visits a website to which the Moving Defendants serve ads, regardless of whether or not a cookie has been set, *see* CAC ¶¶ 30-36, 41, 46, and thus was not "intercepted" within the meaning of the Wiretap Act. *See Yunker*, 2013 WL 1282980, at **7-8

(dismissing Wiretap Act claim where plaintiff provided information at issue to the defendant, which did not constitute "intercept[ion]"). Thus, the only information the Moving Defendants allegedly received "through the use of" the cookies, and that might theoretically meet the statutory definition of "intercepted" information, is the Cookie Values themselves. *See id.* But the Cookie Values are merely unique strings of numbers and letters created not by Plaintiffs but by the party setting the cookie, and sent not by Plaintiffs but by the cookies themselves – so those too cannot be considered communications by *Plaintiffs*, or of *Plaintiffs'* information, that the Moving Defendants in turn "intercepted." *See id.*

Moreover, even if the CAC alleged that the Moving Defendants "intercepted" Plaintiffs' communications (which it does not), Plaintiffs' Wiretap Act claim would still fail. Automatically generated data, such as time of origination, destination and duration of a call are not "contents"; thus the Browser-Generated Information, which besides the URLs consists entirely of such automatically generated data, also is not "contents." *In re iPhone*, 844 F. Supp. 2d at 1061. And there is no principled distinction between a URL and a phone number; both constitute information entered into a device *to permit communication, not* the communication itself. *See, e.g., In re Application of the U.S.*, 416 F. Supp. 2d 13, 18 n.7 (D.D.C. 2006) (holding that "dialing, routing, *addressing*, and signaling information," including originating IP addresses, header information, packet payloads, and the date and times of communications are not "contents") (emphasis added). *See also U.S. v. Polizzi*, 549 F. Supp. 2d 308, 393 (E.D.N.Y. 2008) (holding that no expectation of privacy exists for online transactional information, such as a computer user's Internet search history), *vacated on other grounds*, *U.S. v. Polouizzi*, 564 F. 3d 142 (2d Cir. 2009). Moreover, the Cookie Values, being merely unique strings of numbers and letters created by the party setting the cookie, are clearly not the "contents" of a communication

by Plaintiffs, as they convey no information about the substance, purport or meaning of any communications Plaintiffs may have made. *See Polizzi,* 549 F. Supp. 2d 393.[5]

II. PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE STORED COMMUNICATIONS ACT

Plaintiffs also fail to state a claim under the SCA, which is not a "catch-all statute," *Low v. LinkedIn Corp.*, No. 11-cv-01768-LHK, 2012 WL 2873847, at *6 (N.D. Cal. July 12, 2012), but rather prohibits specific conduct that the CAC's factual allegations do not describe, namely: (i) unauthorized access (ii) of "a facility through which an electronic communications service [(an "ECS")] is provided" (iii) "thereby obtain[ing]. . . a wire or electronic communication" that was not "of or intended for" the person in question (iv) "while it is in electronic storage." 18 U.S.C. §§ 2701(a), (c). Plaintiffs' theory is that (i) the Moving Defendants' alleged setting of cookies was unauthorized "access" of (ii) certain "browser managed files" that were "facilities" through which Plaintiffs' Safari browsers provided an ECS, and (iii) the Moving Defendants "thereby" obtained the Browser Generated Information and Cookie Values, which information was not "of or intended for" them and (iv) was "in electronic storage." These allegations fail to satisfy any of the four listed elements of the SCA.

A. The Moving Defendants' Alleged "Access" Was Not Unauthorized

The alleged setting of the cookies – the means by which the Moving Defendants purportedly "accessed" the browser-managed files – was not "without authorization."[6] Rather,

[5] Plaintiffs conclusorily assert that the Moving Defendants violated Sections 2511(1)(c) and (d) of the Wiretap Act by "disclos[ing]" and "us[ing]" the allegedly improperly intercepted information. CAC ¶ 211(b) and (c). Because they have failed to allege any interception in violation of the Wiretap Act, these additional Wiretap Act claims also fail. *See* 18 U.S.C. § 2511(1)(c)-(d) (creating liability only for use and disclosure of information "obtained in violation of this subsection"). Moreover, the CAC contains no factual allegations indicating what information the Moving Defendants purportedly disclosed or to whom they purportedly disclosed it.

Plaintiffs' own allegations, and the Mayer Article on which they are based, demonstrate that the Moving Defendants set the cookies in a manner *specifically permitted* by the Safari browser itself, in the course of its normal operation and functioning. *See supra* at 3-4 (citing CAC ¶¶ 74-77, 153-154, 161; Coyle Decl. Ex. A at 2-3). Thus, "[P]laintiffs have proffered no proofs whatsoever to support their bare assertion that [the Moving Defendants'] access was unauthorized . . . [and] every fact they do allege supports the inference that the [Safari browser] did authorize [the Moving Defendants'] access." *In re Doubleclick*, 154 F. Supp. 2d at 510.

B. Browsers Are Not ECS Providers And Browser-Managed Files Are Not Facilities Through Which An ECS Is Provided

Even if the alleged cookie-setting constituted unauthorized access of the browser-managed files, which it does not, the SCA claim would still fail because browsers are not ECS providers and browser-managed files are not "facilities" through which an ECS is provided. The SCA defines an "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (incorporated by reference in the SCA, 18 U.S.C. § 2711(1)). Plaintiffs do nothing more than parrot this language in making the conclusory assertion that their Safari browsers are ECS providers, and fail to cite a single case in support of this nonsensical theory. CAC ¶ 216. Traditional examples of ECS providers are telephone companies, internet or e-mail service providers, and bulletin board services, *see, e.g.*, *Garcia v. City of Laredo, Tex.*, 702 F. 3d 788, 792 (5th Cir. 2012), and Plaintiffs allege no facts explaining how "web-browser software" is in any way analogous to these entities. CAC ¶¶ 28, 68. Moreover, courts have consistently held

[6] The SCA does not define the phrase "without authorization." Courts considering the issue have drawn an analogy with the phrase "exceeds authorized access" in the CFAA, which means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6); *see Penrose Computer Marketgroup, Inc. v. Camin*, 682 F. Supp. 2d 202, 211 (N.D.N.Y. 2010); *Cheng v. Romo*, No. 11-10007-DJC, 2012 WL 6021369, at *3 n.3 (D. Mass. Nov. 28, 2012).

that neither the users of an ECS nor their individual computers or mobile devices are ECS providers. *Garcia*, 702 F. 3d 792-793 (5th Cir. 2012) ("personal cell phone does not *provide* an [ECS] just because the device *enables use of* [an ECS]") (emphasis in original).[7] If a user's computer or mobile device cannot be an ECS provider under the SCA, then certainly software residing on the device also cannot.

Equally unavailing is Plaintiffs' allegation that the "browser-managed files" in which Safari allegedly stores cookies and other information constitute "facilit[ies]" within the meaning of the SCA. CAC ¶ 217. Although the SCA does not define the term "facility," it requires that a covered facility be something "*through which an electronic communication service is provided*." 18 U.S.C. § 2701(a) (emphasis added). But Plaintiffs nowhere explain how a browser, to the extent it "provides" internet access at all (which it does not), purportedly provides such access "*through*" browser managed files. Moreover, "the relevant facilities that the SCA is designed to protect . . . are facilities that are *operated by* [ECS] providers." *Freedom Banc Mortg. Servs., Inc. v. O'Harra*, No. 2:11-cv-01073, 2012 WL 3862209, at *9 (S.D. Ohio Sept. 5, 2012) (emphasis added). Even if Safari browsers were ECS providers, which they are not, it is nonsensical to speak of a file being "operated by" a browser the way that a server is "operated by" an internet service provider.

[7] *See also United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003) (SCA does not apply to individual computer user's hard drive); *In re DoubleClick*, 154 F. Supp. 2d at 512 (legislative history shows that SCA "makes no mention of individual users' computers"); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 524 (N.D. Ill. 2011) (holding that an ECS provider supplies "the underlying service which transports the data . . . [and is] not the provider of a product or service which facilitate[s] the data transport").

C. The Moving Defendants Did Not Receive The Browser-Generated Information By Means Of Their Alleged Cookie-Setting, And They Were Legally Authorized To Receive The Cookie Values

Even if the alleged cookie setting was unauthorized (which it was not) and the browser-managed files were facilities through which Plaintiffs' browsers provided an ECS (which they were not), the Moving Defendants cannot have obtained the Browser-Generated Information as a result of such access. Rather, Plaintiffs specifically allege that their browsers sent the Browser-Generated Information directly to the Moving Defendants each time they requested an ad, *regardless of whether the browser contained a cookie*. *See* CAC ¶¶ 30-36, 41, 46. Indeed, the court in *Crowley*, faced with precisely the same facts, held that the defendant, Amazon, had not "*access[ed]*" plaintiffs' computer *at all*, notwithstanding plaintiffs' "conclusory allegation to that effect," because the plaintiff had "sent his information to Amazon electronically." 166 F. Supp. 2d at 1271-72 (emphasis added). Like the complaint in *Crowley*, the facts alleged in the CAC do not show that the Moving Defendants "gain[ed] access to [Plaintiffs'] computer[s] in order to obtain the . . . [Browser Generated Information]," but rather that the Moving Defendants "received a voluntary transmission of [such] information from [Plaintiffs' browsers]." *Id.*

Moreover, although the Plaintiffs claim that the Cookie Values were obtained by the Moving Defendants as a result of the alleged cookie-setting, this does not help Plaintiffs, as conduct that would otherwise fall within the SCA's boundaries is not actionable if it was authorized by a "user" of the relevant ECS with respect to a communication "of or intended for" that user. *See* 18 U.S.C. § 2701(c). To the extent Plaintiffs' browsers were ECS providers, the Moving Defendants were "users" of the ECS that the browsers provided (internet access), and "[p]utting aside the issue of whether the cookie identification numbers are electronic communications *at all*," the Moving Defendants "did not need anyone's authority to access them," because they were the Moving Defendants' "internal . . . communications" and thus were

both "of" and "intended for" the Moving Defendants. *In re Doubleclick*, 154 F. Supp. 2d at 511-13 (emphasis added); *see also In re iPhone*, 844 F. Supp. 2d at 1058 (holding that, assuming *arguendo* plaintiffs' iPhones were facilities, the apps that allegedly improperly collected plaintiffs' information were "users" of the service for whom the communications were intended).

D. The Moving Defendants Did Not Obtain Any Electronic Communications While They Were "In Electronic Storage"

Finally, even if (i) the alleged cookie-setting constituted unauthorized access of the browser-managed files (which it did not); (ii) the browser-managed files were facilities through which the browsers provided an ECS (which they were not); and (iii) either the Moving Defendants obtained the Browser-Generated Information as a result of that access (which they did not), or the Cookie Values were not "of" and "intended for" the Moving Defendants as "users" of the ECS the browsers allegedly provided (which they were), the SCA claim would still fail because (iv) neither the Browser-Generated Information nor the Cookie Values were "in electronic storage" as that term is defined in the SCA when they were allegedly obtained by the Moving Defendants.

The SCA defines "electronic storage" as "(a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17) (incorporated by reference in the SCA, 18 U.S.C. § 2711(1)). Courts have consistently held that information stored on an individual's personal computing device – as Plaintiffs allege here – is not in electronic storage. *See In re Doubleclick*, 154 F. Supp. 2d at 512 (holding that SCA's "language and legislative history make evident that 'electronic storage' [was] not meant to include [defendant ad-serving company's] cookies"); *Yunker*, 2013 WL 1282980, at **8-9 (holding that neither unique device

ID number, which plaintiffs described as a "supercookie," nor information plaintiffs sent directly to defendant, were in "electronic storage" for purposes of SCA claim).[8] But even were that not the rule, Plaintiffs still would have no SCA claim, because Plaintiffs' allegation that the Cookie Values and Browser-Generated Information were accessed out of their computers' random access memory, or "RAM," CAC ¶ 218, is directly contradicted by other allegations in the CAC: Plaintiffs start by alleging that this information was accessed upon being received by the Moving Defendants, CAC ¶ 41; they later say it was intercepted while it was "in transit" to first-party websites. CAC ¶ 208.

Finally, even if the Browser-Generated Information and the Cookie Values were accessed when they were in "temporary storage" (which they were not), Plaintiffs nowhere allege facts showing that such storage was "*intermediate*" storage, *i.e.*, that at the time the Browser-Generated Information and Cookie Values were accessed, they were being "stored 'for a limited time' *in the 'middle' of a transmission*." *In re Doubleclick*, 154 F. Supp. 2d at 512 (emphasis added). To the contrary, to the extent the Browser-Generated Information and Cookie Values were accessed while in Plaintiffs' computers' RAM, that access would by definition be prior to, as opposed to "in the middle of," any transmission.

III. PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE CFAA

To assert a private right of action under the CFAA, Plaintiffs must allege "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value," that occurred

[8] *See also Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183, 1205 (S.D. Cal. 2008) (emails stored on laptop computer not in "temporary, intermediate storage" under SCA); *Bailey v. Bailey*, No. 07-11672, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008) (SCA does not extend to information "stored only on Plaintiff's personal computer"); *Thompson v. Ross*, No. 2:10-cv-479, 2010 WL 3896533, *5 (W.D. Pa. Sept. 30. 2010) (communications "downloaded and stored on, and subsequently accessed solely from, a user's personal computer does not fit within the SCA's definition of electronic storage."); *Garcia*, 702 F.3d at 793 (information stored to computer hard drive or cell phone not in electronic storage).

"by reason of a violation of [Section 1030]." 18 U.S.C. §§ 1030(c)(4)(A)(I), 1030(g). Plaintiffs contend that the Moving Defendants violated § 1030(a)(2)(C), which proscribes "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer." CAC ¶ 224.[9] Because Plaintiffs fail to allege that they suffered *any* "loss" – much less $5,000 worth of loss – and that the Moving Defendants accessed Plaintiffs' computers "without authorization" or "exceed[ed] authorized access," their CFAA claim should be dismissed.

A. Plaintiffs Do Not Allege That They Suffered Any "Loss," Much Less A $5,000 Loss

The CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages because of interruption of service." 18 U.S.C. § 1030(e)(11). Only "economic damages" qualify as CFAA "losses." § 1030(g); *see also Creative Computing v. Getloaded, LLC*, 386 F. 3d 930, 935 (9th Cir. 2004). Plaintiffs fail to plead that they incurred a single dollar in "costs" or suffered even one moment of interrupted service as a result of the Moving Defendants' alleged conduct.

In particular, Plaintiffs' generalized allegations about the purported economic value of their personal information, CAC ¶¶ 49-67, do not suffice to plead a loss of revenue. As an initial matter, Plaintiffs plead no facts from which an inference can be drawn that the Moving

[9] The CAC also cites to Sections 1030(a)(5)(a)(i) and (iii), CAC ¶¶ 225-226; however these provisions do not exist. To the extent Plaintiffs intended to allege violations of Sections 1030(a)(5)(A) and (C), which proscribe, respectively: (i) "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization"; and (ii) "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss," the CFAA claim fails for the same reasons discussed *infra*.

Defendants collected any of their personally identifying information. Plaintiffs' conclusory assertions to that effect, *see* CAC ¶¶ 3, 67, 156-158, 161, are unsupported by any facts alleged in the CAC, and are instead based entirely on Plaintiffs' allegations that *Google* routinely receives personally identifying information from its users. CAC ¶¶ 97-98, 112-113.

In stark contrast to the detailed allegations regarding the types of personally identifying information Google collects and when and how Google collects it, however, Plaintiffs allege *no facts* indicating that *the Moving Defendants* ever collected users' names, addresses, or any other personally identifying information. *Compare* CAC ¶¶ 57-59, 89, 96-98, 101, 112-113, 121-123, *with id*. ¶¶ 158, 161. This is unsurprising. As detailed in the CAC, Google offers a number of popular services – including Gmail and Google+ – that users may access without charge by providing Google with detailed personal information and agreeing that such information may be used in accordance with certain terms and conditions. CAC ¶¶ 14, 57-59, 97-98, 101, 112-113, 121-123, 164; Coyle Decl. Ex. A at 3. Plaintiffs do not allege that the Moving Defendants provided any such services to internet users or engaged in any other activity that would entail the collection of personal information.

Moreover, even if Plaintiffs had alleged facts in support of their conclusory statement that the Moving Defendants collected their personal information, which they have not, "it is not enough to allege that [Plaintiffs'] information has value to [the Moving Defendants]; the term 'loss' requires that Plaintiffs suffer a detriment—a detriment amounting to more than $5,000." *Del Vecchio v. Amazon.com, Inc.*, No. 11-366, 2012 WL 1997697, at *4 (W.D. Wash. June 1, 2012) (emphasis in original). Courts have consistently dismissed complaints alleging CFAA "loss" arising from the collection or use of, or access to, personal information. *See, e.g., In re*

iPhone, 844 F. Supp. 2d at 1068.[10] *Cf. La Court v. Specific Media*, No. 10-1256, 2011 WL 1661532, at *4-5 (C.D. Cal. Apr. 28, 2011) (dismissing case for failure to allege injury in fact where plaintiffs merely referred "to a number of academic articles" but did not actually identify "a single individual who was foreclosed from entering into a 'value-for-value exchange' as a result of [defendant's] alleged conduct").[11]

Finally, even if Plaintiffs had pled some cognizable, *de minimis* individual losses (which they have not), they could not aggregate those losses across the putative class to satisfy the CFAA's $5,000 loss requirement. The CFAA permits aggregation of losses resulting from "a related course of conduct affecting" more than one computer "*only*" in the case of "an investigation, prosecution, or other proceeding *brought by the United States*," *i.e., not* in the case of a private civil action. 18 U.S.C. § 1030(c)(4)(A)(i)(I) (emphasis added). Thus, in the civil litigation context, such aggregation is only permitted in connection with a "single act," and "the definition of a prohibited act turns on the perpetrator's access to a *particular* computer." *DoubleClick*, 154 F. Supp. 2d at 525; *see also Bose*, 2011 WL 4343517, at *6-7. In other words,

[10] *See also In re Zynga Privacy Litig*., No. C-10-04680 JWW, 2011 WL 7479170, at *1(N.D. Cal June 15, 2011); *In re DoubleClick Inc. Privacy Litig*., 154 F. Supp. 2d 497, 525 (S.D.N.Y 2001); *Bose v. Interclick, Inc.*, No. 10-9183, 2011 WL 4343517, at *6-7 (S.D.N.Y. Aug. 17, 2011).

[11] Because Plaintiffs' claims against the Moving Defendants all fail under Fed. R. Civ. P. 12(b)(6), the Court need not decide whether Plaintiffs lack Article III standing based on their above-described inability to allege any injury-in-fact. If the Court were to reach this issue, it would have to decide whether the Third Circuit's decision in *Alston v. Countrywide Fin. Corp.*, 585 F.3d 753, 763 (3d Cir. 2009), should be read to hold that Article III standing can be predicated solely upon an alleged federal statutory violation, even without any allegation of separate injury stemming from such violation, notwithstanding the Supreme Court's admonition in *Warth v. Seldin*, 422 U.S. 490, 501 (1975), that even where a statutory violation is alleged, "Art[icle] III's requirement remains: the plaintiff still must allege a distinct and palpable injury to himself." Further Supreme Court guidance on this hotly debated issue will likely be forthcoming very soon. *See U. S. Forest Serv. v. Pacific Rivers Council*, 133 S. Ct. 1582 (2013) (granting petition for writ of certiorari on Ninth Circuit's Article III standing decision in *Pacific Rivers Council v. U. S. Forest Service*, 689 F.3d 1012 (9th Cir. 2012)).

"the suggestion that [the Moving Defendants' alleged] accessing of cookies on millions of plaintiffs' computers could constitute a single act is refuted by the statute's plain language," *Doubleclick*, 154 F. Supp. 2d at 524 (emphasis in original), and Plaintiffs' allegation that the Moving Defendants improperly set cookies on the computers of "tens of millions of people" therefore prevents them from aggregating any alleged loss across members of the putative class. CAC ¶ 75; *see also id.* ¶¶ 74, 193.

B. Plaintiffs Do Not Allege That The Moving Defendants Committed Any Violation Of Section 1030

Even if Plaintiffs were able to satisfy the CFAA's $5,000 damages threshold (which they are not), their CFAA claim would still fail because they do not allege that the Moving Defendants acted "without authorization" or "exceed[ed] authorized access," as they must to plead a violation under Section 1030. *See* 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(5)(A), 1030(a)(5)(C).[12]

1. Plaintiffs Do Not Allege That The Moving Defendants Acted "Without Authorization"

A 'person uses a computer 'without authorization'" only if "the person has not received permission to use the computer *for any purpose*" or if the owner "has rescinded permission to access the computer and the defendant uses the computer anyway." *LVRC Holdings v. Brekka*, 581 F. 3d 1127, 1135 (2009) (emphasis added). Because the CFAA is a criminal statute, courts must read the term "without authorization" narrowly to provide adequate notice of the prohibited

[12] The CAC also fails to state a violation under Section 1030(a)(5) for other, independent reasons. First, Plaintiffs' failure to plead any "damage," which the CFAA defines as "impairment to the integrity or availability of data, a program, a system, or information," 18 U.S.C. § 1030(e)(8), is fatal to any claim that the Moving Defendants violated either Section 1030(a)(5)(A) or Section 1030(a)(5)(C). Second, Plaintiffs' failure to plead any facts to support an inference that the Moving Defendants intended to cause damage to Plaintiffs' computers is fatal to any attempt to plead a violation of 1030(a)(5)(A). *See Kalow v. Springnut, LLP v. Commence Corp.*, No. 07-3442, 2008 WL 2557506, at *4 (D.N.J. June 23, 2008) (dismissing CFAA claim where plaintiff failed to allege "actual intent").

conduct and avoid unconstitutional vagueness. *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F. 3d 199, 204 (4th Cir. 2012) (quoting *U.S. v. Nosal*, 676 F. 3d 854, 856); *see also CBS Corp. v. FCC*, 663 F. 3d 144, 174 n.19 (3d Cir. 2011).

Plaintiffs admittedly granted the Moving Defendants permission to access their computers for *some* purpose when they directly requested that the Moving Defendants send them an ad to be displayed on their monitor. CAC ¶ 41. Thus, the alleged cookie-setting could not have been "without authorization" within the meaning of the CFAA. *See Brekka*, 581 F. 3d at 1135. Plaintiffs' purported belief that the Partial-Allowance Setting would not allow a cookie to be set by a domain that the browser had not visited, CAC ¶ 69-72, does not alter this analysis. By employing the Partial-Allowance Setting, Plaintiffs granted permission for cookies to be set if, and to the extent, the Partial-Allowance Setting's code permitted. *See In re iPhone*, 844 F. Supp. 2d at 1066-68 (holding that defendants had not accessed plaintiffs' devices without authorization where plaintiffs had voluntarily downloaded software that allegedly collected their personal information without their knowledge). As discussed above, the Mayer Article itself demonstrates that the Partial-Allowance Setting specifically permitted cookies to be set in precisely the manner in which the Moving Defendants allegedly set them. *See supra* at 3-4 (citing CAC ¶¶ 74-77, 153-154, 161; Coyle Decl. Ex. A at 2-3).

2. Plaintiffs Do Not Allege That The Moving Defendants "Exceed[ed] Authorized Access" To Their Computers

The CAC also fails to state a violation of the CFAA based on the Moving Defendants having "exceed[ed] authorized access" to Plaintiffs' computers, because it alleges no facts showing that the Moving Defendants "used [authorized] access [to Plaintiffs' computers] to obtain or alter information in the computer that [the Moving Defendants were] not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). As discussed above, the only item allegedly received

by the Moving Defendants as a result of the alleged cookie-setting was the Cookie Values, *see supra* at 7-8, which they were clearly entitled to obtain. *See In re Doubleclick*, 154 F. Supp. 2d at 511-13 (ad-serving company's cookies are both "of" and "intended for" the ad-serving company).

CONCLUSION

For all of the foregoing reasons, Moving Defendants respectfully request that the Court dismiss all of the claims asserted against the Moving Defendants in the CAC.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Regina S.E. Murphy

Rodger D. Smith II (#3778)
Regina S.E. Murphy (#5648)
1201 North Market Street, 18th Floor
P.O. Box 1347
Wilmington, Delaware 19899-1347
(302) 658-9200
rsmith@mnat.com
rmurphy@mnat.com

Attorneys for Defendants Media Innovation Group, LLC and WPP plc

OF COUNSEL:

Douglas H. Meal
Lisa M. Coyle
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
(617) 951-7000

May 1, 2013

CERTIFICATE OF SERVICE

I hereby certify that on May 1, 2013, I caused the foregoing to be electronically filed with the Clerk of the Court using CM/ECF, which will send notification of such filing to all registered participants.

I further certify that I caused copies of the foregoing document to be served on May 1, 2013, upon the following in the manner indicated:

Stephen G. Grygiel, Esquire — *VIA ELECTRONIC MAIL*
KEEFE BARTELS
170 Monmouth Street
Red Bank, NJ 07701
Interim Lead Counsel for the Putative Plaintiff Class

Brian Russell Strange, Esquire — *VIA ELECTRONIC MAIL*
STRANGE & CARPENTER
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Interim Lead Counsel for the Putative Plaintiff Class

James Frickleton, Esquire — *VIA ELECTRONIC MAIL*
BARTIMUS, FRICKLETON, ROBERTSON & GORNY-LEAWOOD
11150 Overbrook Road, Suite 200
Leawood, KS 66211
Interim Lead Counsel for the Putative Plaintiff Class

Seth D. Rigrodsky, Esquire — *VIA ELECTRONIC MAIL*
Brian D. Long, Esquire
Gina M. Serra, Esquire
RIGRODSKY & LONG, P.A.
2 Righter Parkway, Suite 120
Wilmington, DE 19801
Council for Proposed Intervening Plaintiffs Daniel Mazzone, Michelle Kuswanto, Michael Frohberg and Andy Wu

Kim E. Richman, Esquire — *VIA ELECTRONIC MAIL*
Michael R. Reese, Esquire
George Granade, Esquire
REESE RICHMAN LLP
875 Avenue of the Americas, 18th Floor
New York, NY 10001
Council for Proposed Intervening Plaintiffs Daniel Mazzone, Michelle Kuswanto, Michael Frohberg and Andy Wu

Sanford P. Dumain, Esquire — *VIA ELECTRONIC MAIL*
Adam Bobkin, Esquire
Melissa Clark, Esquire
Leigh Smith, Esquire
MILBERG LLP
One Penn Plaza
New York, NY 10119
Council for Proposed Intervening Plaintiffs Daniel Mazzone, Michelle Kuswanto, Michael Frohberg and Andy Wu

David Azar, Esquire — *VIA ELECTRONIC MAIL*
MILBERG LLP
300 South Grand Avenue, Suite 3900
Los Angeles, CA 90071
Council for Proposed Intervening Plaintiffs Daniel Mazzone, Michelle Kuswanto, Michael Frohberg and Andy Wu

Kelly E. Farnan, Esquire — *VIA ELECTRONIC MAIL*
Rudolf Koch, Esquire
Travis S. Hunter, Esquire
RICHARDS, LAYTON & FINGER P.A.
920 North King Street
Wilmington, Delaware 19801
Attorneys for Defendant Vibrant Media Inc.

Edward P. Boyle, Esquire — *VIA ELECTRONIC MAIL*
David N. Cinotti, Esquire
Joeann E. Walker, Esquire
VENABLE LLP
1270 Avenue of the Americas, 24th Floor
New York, NY 10020
Attorneys for Defendant Vibrant Media Inc.

Anthony J. Weibell, Esquire *VIA ELECTRONIC MAIL*
WILSON SONSINI GOODRICH & ROSATI
650 Page Mill Road
Palo Alto, CA 94304-1050
Attorneys for Defendant Google Inc.

Carol Lynn Thompson, Esquire *VIA ELECTRONIC MAIL*
SIDLEY AUSTIN LLP
555 California Street, 20th Floor
San Francisco, CA 94104
Attorneys for Defendant Pointroll Inc.

/s/ Regina S.E. Murphy

Regina S.E. Murphy (#5648)